

Domande LAS

Introduzione al corso

1. Le certificazioni professionali in ambito Linux sono utili sul mercato del lavoro.
2. L'amministratore di sistema non ha responsabilità legali, solo operative.
3. È consigliabile che l'amministratore effettui il login come root, in quanto la maggior parte delle attività richiedono i privilegi corrispondenti.

Shell scripting

4. Gli alias di bash possono contenere altri alias, che vengono espansi.
5. Gli alias di bash possono espandersi ricorsivamente se stessi.
6. Le pagine di manuale sono divise in sezioni.
7. Non possono esistere due man page con lo stesso nome.
8. Un comando invocato col nome "nudo" del programma (esempio: ls) viene eseguito da bash di default se trovato nella directory corrente.

Device filesystem

9. I device driver rispettano le interfacce delle system call standard (open, close, read, ...) e implementano i comandi corretti per il corrispondente dispositivo.

10. I file in /dev contengono una copia dei dati dei rispettivi dispositivi.

11. Un disco può essere formattato senza essere partizionato.

12. Un disco e una sua partizione sono entrambi dispositivi a blocchi.

13. I file di un filesystem possono essere acceduti direttamente con la notazione /dev/partizione/percorso/file.

14. I file in /dev corrispondono uno-a-uno coi device installati sul sistema.

Gestione servizi

15. I log non possono essere analizzati in tempo reale.

16. I target di systemd sono grosso modo equivalenti ai runlevel di SysVinit.

17. Il carico riportato da uptime rappresenta la percentuale di utilizzo della CPU.

18. df e du sono strumenti differenti per ottenere la stessa informazione.

19. Il selettor local1.info cattura anche messaggi con etichette diverse.

20. La direttiva WantedBy nella definizione di una unit di servizio agisce quando il servizio viene avviato.

21. La pianificazione di attività con cron è riservata all'utente root.

22. La pianificazione di attività con cron ha un periodo minimo di un minuto.

23. L'azione disable di systemctl impedisce completamente l'avvio del servizio.

24. Le azioni start e stop di systemctl agiscono istantaneamente sul servizio.

25. Le facility di syslog sono un insieme non ordinato.

26. Se uptime riporta 0.70 0.35 0.88 come valori medi del carico, ciò indica un picco di carico avvenuto di recente e superato.

27. top è comando più adatto per catturare una "fotografia istantanea" dello stato dei processi in formato flessibile per successive elaborazioni.

28. Un processo può essere avviato in tre modi: lancio da parte di un utente, avvio al boot da parte di systemd, esecuzione periodica attraverso cron. ●

29. Un servizio di tipo oneshot di systemd può risultare attivo anche se non corrisponde ad alcun processo in esecuzione. ●

30. Uno dei vantaggi di utilizzare un sistema di logging centralizzato è la marcatura temporale coerente dei messaggi. ●

31. top riassume in una schermata l'output di free, ps, uptime. ●

32. syslog classifica i messaggi principalmente sulla base del contenuto. ●

33. lsof permette, in certe condizioni, di individuare file cancellati. ●

34. La CPU troppo lenta può non essere la causa principale di accodamento di processi e conseguente aumento del carico. ●

35. un task pianificato con cron come 10 22 2,20 * 4 viene eseguito almeno 6 volte al mese. ●

36. Il sistema di logging integrato in systemd è avviato prima di syslogd. ?

Utenti e file

37. Il comando sudo permette di differenziare quali comandi un utente può eseguire coi privilegi di un altro utente.

38. La possibilità di cancellare un file è determinata unicamente dai permessi assegnati alla directory che lo contiene.

39. Ogni file ha come unico proprietario un utente.

40. Il comando sudo richiede all'utente la password di root per autorizzare l'esecuzione privilegiata di comandi.

41. Senza permesso di lettura su di una directory, non si possono utilizzare i file in essa contenuti.

Alta disponibilità

42. Il vantaggio dei sistemi NAS su quelli SAN è che non richiedono coordinazione tra i client.

43. Nell'architettura LVM, un Logical Volume viene costruito in modo da presentare un elenco di blocchi contigui anche se fisicamente utilizza blocchi sparsi.

44. Nell'architettura LVM, un Physical Volume viene utilizzato analogamente a una tradizionale partizione di un disco.

45. Ripristinare l'integrità di un RAID dopo la sostituzione di un disco può richiedere vari giorni.

46. Una disponibilità a "6 nove" è facilmente ottenibile con una coppia di computer configurati con heartbeat per il failover automatico.

47. Un sistema di storage ideale (totalmente resistente a qualsiasi guasto hardware) rende superfluo fare backup.

48. Il downtime riconducibile a problemi software è superiore a quello imputabile a guasti hardware.

49. Tutti i livelli RAID da 0 a 6 aumentano la tolleranza ai guasti.

50. I sistemi NAS sono più efficienti dei sistemi SAN.

Gestione dei pacchetti software

51. yum e apt sono strumenti per la gestione dei pacchetti Debian (e distribuzioni derivate).

52. Solo il produttore di una distribuzione può realizzare pacchetti installabili correttamente su di un sistema che l'abbia adottata.

53. dpkg risolve automaticamente le dipendenze in fase di installazione di un pacchetto.

54. Una distribuzione LTS differisce da una standard per la durata del supporto offerto dal produttore.

55. L'installazione manuale da sorgenti è più flessibile rispetto all'installazione da binari precompilati.

Networking di base

56. Gli indirizzi nel range 169.254.1.0 – 169.254.254.255 sono riservati all'allocazione automatica link local.

57. La configurazione di un'interfaccia col comando ip a add 10.1.1.5/24 dev eth1 assegna un indirizzo in modo persistente.

58. L'assegnamento di un indirizzo IPv4 link local avviene prima di interrogare server che potrebbero assegnare un indirizzo diverso all'host.

59. L'assegnamento di un indirizzo IPv6 link local secondo il modello SLAAC avviene prima di interrogare server che potrebbero assegnare un indirizzo diverso all'host.

60. NSS (Name Service Switch) è il sistema per la risoluzione dei nomi host in indirizzi IP.

61. Gli standard promossi dallo Zeroconf Working Group permettono di configurare automaticamente i protocolli da usare a tutti i livelli, da quello fisico a quello applicativo.

62. Il comando ss non è in grado di riportare alcuna informazione sul traffico che fluisce attraverso un router.

63. Il comando `tcpdump` non permette di rilevare se un processo è in ascolto su di una porta TCP.

64. Il comando `ip a add 10.1.1.5/24 dev eth1` modifica anche la tabella di instradamento del sistema.

65. I nomi assegnati nel dominio `.local` sono tipicamente strutturati in modo gerarchico secondo le esigenze dell'organizzazione aziendale.

66. `dnsmasq` può essere lanciato in più istanze per servire richieste su interfacce diverse con configurazioni incompatibili tra loro.

67. NTP consente la sincronizzazione via Internet con errori ben inferiori al secondo.

Monitoraggio centralizzato

68. Attraverso le definizioni SMI, è possibile definire strutture dati di complessità arbitraria per managed object di SNMP.

69. Nel sottoalbero del MIB con origine `.1.3.6.1.4.1` qualsiasi ente può richiedere un ramo privato.

70. Si definisce agent qualsiasi dispositivo fisico connesso in rete che supporti il protocollo SNMP.

71. SNMP è un protocollo applicativo trasportato su UDP.

72. SNMP è utilizzabile per il monitoraggio di dispositivi, ma è principalmente impiegato per la loro configurazione.

73. Solo la versione 3 di SNMP prevede sistemi di sicurezza robusti.

74. In SNMP l'interazione tra manager e agent è sempre del tipo richiesta-risposta.

75. Il MIB teoricamente è un modello per collocare in una tassonomia qualsiasi tipo di informazione.

Configurazione centralizzata

76. I tipi di attributo fondamentali per l'organizzazione delle entry LDAP per l'autenticazione sono dc, ou, cn, uid.

77. Il modello multimaster consente modifiche simultanee dello stesso database LDAP su diversi server.

78. LDAP è essenzialmente un database specializzato per distribuire informazioni relative a utenti.

79. LDAP utilizza un modello relazionale dei dati.

80. Le entry LDAP possono essere trovate solamente conoscendo il loro Distinguished Name.

81. Una Object Class non è altro che la specifica di quali tipi di attributo siano necessari o ammessi in una entry che la istanzia.

82. Il Distinguished Name identifica una entry LDAP ma non la sua posizione nel DIT.

83. Le entry di LDAP possono essere mostrate secondo differenti organizzazioni gerarchiche.

84. Gli attributi di una entry LDAP sono come variabili a cui viene assegnato un singolo valore.

85. LDAP è un sistema autonomo che fornisce tutti i componenti necessari per l'autenticazione centralizzata di utenti.

86. Una entry LDAP può essere istanza di più classi simultaneamente.